(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 716 021**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **94 01463**

(51) Int Cl[6] : G 06 K 19/073, 7/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 09.02.94.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 11.08.95 Bulletin 95/32.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s)** : *Société anonyme dite GEMPLUS CARD INTERNATIONAL* — FR.

(72) **Inventeur(s)** : Valadier Jean-Louis.

(73) **Titulaire(s) :**

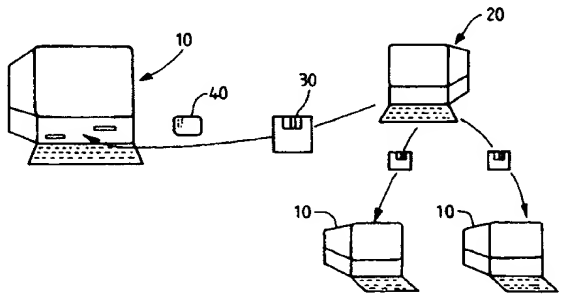
(74) **Mandataire** : Cabinet Ballot-Schmit.

(54) Procédé et système de transaction par carte à puce.

(57) L'invention concerne les transactions utilisant les cartes à puces.

Pour permettre de sécuriser simplement des opérations de rechargement de montants prépayés dans des cartes à mémoire, même à partir de terminaux (10) dispersés non reliés à un serveur central (20), on propose selon l'invention de mémoriser dans la carte à mémoire (40) le nombre d'opérations de rechargement effectuées. Un compteur de nombre de rechargements est donc prévu; ce compteur est incrémenté à chaque rechargement mais n'est pas incrémenté lors des autres utilisations de la carte, et notamment lors de l'utilisation de celle-ci pour consommer des biens ou services.

L'invention est particulièrement applicable à la gestion collective de nombreux restaurants d'entreprise ayant chacun plusieurs terminaux de rechargement à la disposition des employés de l'entreprise.



FR 2 716 021 - A1

PROCEDE ET SYSTEME DE TRANSACTION PAR CARTE A PUCE

L'invention concerne les cartes à puces et les systèmes de transaction utilisant ces cartes. Les puces de ces cartes peuvent être des puces avec mémoire seule ou bien des puces comportant une mémoire et un microprocesseur. On peut même envisager d'avoir au moins deux puces, une mémoire et un microprocesseur, sur la même carte.

Un système de transaction avec carte à puce typique est le porte monnaie électronique qui fonctionne de la manière suivante : une carte à puce d'un particulier peut être rechargée auprès d'une institution bancaire pour contenir une nouvelle valeur fiduciaire remplaçant des billets de banque, le compte en banque du particulier étant débité d'une valeur correspondante; cette carte peut être utilisée pour un échange d'argent avec un tiers (un commerçant par exemple) ayant une carte similaire : une partie de l'argent disponible dans la première carte est mise au crédit de la deuxième dont le solde est ainsi augmenté; le solde de la première carte est diminué d'autant. Après un certain nombre d'opérations de ce genre, la deuxième carte peut être déchargée auprès d'une institution bancaire pour transférer le solde de la carte vers un compte du titulaire de cette carte.

Un autre système de transaction peut consister à recharger des cartes périodiquement à des bornes de rechargement réparties dans une zone géographique, puis à consommer des biens ou des services à l'aide de la carte; le solde de la carte décroît au fur et à mesure de l'utilisation jusqu'à épuisement du montant

rechargé. Le montant rechargé périodiquement peut être fixe ou variable. Il peut être le même pour toute une population de titulaires de cartes, par exemple dans une application où on recharge des cartes de restaurant d'entreprise en début du mois avec un nombre de repas fixe ou une somme d'argent fixe.

D'autres systèmes de transaction situés dans l'esprit de l'invention pourraient concerner uniquement des transferts d'informations sans transfert de valeur monétaire.

Les systèmes de transaction, aussi bien d'unités de valeur que d'informations, exigent en général des précautions contre les fraudes. Pour cela, on utilise des informations confidentielles, des codes secrets, des algorithmes de vérification de codes secrets, des algorithmes de cryptage d'informations, etc.

Dans la demande de brevet FR-A-2653648 du déposant, on a décrit des systèmes de transaction sécurisée, pour des cartes à puces ne comportant pas nécessairement de microprocesseur. Essentiellement, la carte est une carte à mémoire dans laquelle la mémoire non volatile comporte au moins quatre zones différentes. Une première zone est réservée à des données d'identification de la carte (il n'y a en principe pas deux cartes ayant les mêmes données d'identification). Une deuxième zone est réservée à un solde de compte, qui diminue au fur et à mesure des utilisations. Une troisième zone enregistre le nombre d'opérations effectuées avec la carte. Et une quatrième zone contient un certificat servant à vérifier que le solde de la carte n'a pas été modifié entre deux opérations. Le certificat est placé dans cette quatrième zone par le lecteur de carte à l'issue d'une transaction; il est calculé en faisant intervenir l'identité de la carte, le solde, et le nombre d'opérations. Lors d'une utilisation suivante de la

carte, le lecteur de carte vérifie, à l'aide du même algorithme, que le certificat est bien celui qui correspond à l'identité de la carte, au solde inscrit, et au nombre d'opérations inscrit. Si ce n'est pas le cas, il prend des mesures en rapport avec la violation détectée; par exemple il interdit toute transaction, ou il conserve la carte, ou il transmet à un serveur central l'identité de la carte, etc. Cette quatrième zone n'est indispensable que pour les cartes à mémoire. En effet, pour les cartes à mémoires et à micro-processeur la sécurité est basée sur un certificat ou une signature émise par le terminal lors d'un débit ou d'un rechargement de la carte et qui permet à la carte de vérifier l'origine du débit ou du rechargement. De même la vérification de cette zone certificat ne doit être faite pas le terminal que pour les cartes à mémoire car pour les cartes à micro-processeur la valeur du solde peut être garantie par les mécanismes sécuritaires mis en place pour les débits et les rechargements.

Bien que ce système soit très simple et donne une bonne sécurité, on s'est aperçu qu'il présentait des inconvénients pour certaines organisations de systèmes de transaction.

Par exemple, une organisation de transaction dans lequel ce mode de sécurité présente des inconvénients est la suivante : lorsque les utilisateurs doivent recharger leur carte auprès d'une institution, à partir de terminaux de rechargement répartis dans une zone géographique déterminée et reliés à un serveur central, les vérifications sont faites par le serveur, et cela occupe beaucoup de temps de transmission en ligne si les utilisateurs sont nombreux. S'ils doivent tous recharger leurs cartes à peu près au même moment, par exemple en début de mois, le problème est encore plus délicat. Il s'agit là d'un système de rechargement en

liaison directe ("on-line" en anglais); la carte, le terminal de rechargement et le serveur sont en effet reliés entre eux pendant la transaction.

On a donc eu l'idée qu'on pourrait faire par avance les opérations de vérification dans le serveur, à partir des données provenant des opérations précédemment effectuées par les cartes, et qu'on pourrait alors enregistrer dans les terminaux de rechargement tous les certificats des cartes qui peuvent se présenter. Les rechargements sont effectués en différé ("off-line" en anglais), le terminal n'étant pas en communication avec le lecteur au moment du rechargement. Mais cela impose de n'utiliser pour l'algorithme de vérification que des données connues par avance par le serveur. Or le nombre d'opérations effectuées par la carte n'est pas connu, pas plus que le solde du compte. Par conséquent, on ne peut pas appliquer telle quelle la procédure décrite dans la demande de brevet précédemment citée.

La présente invention propose une solution simple pour obtenir une sécurité satisfaisante pour beaucoup d'applications, sans empêcher d'utiliser certaines organisations de transaction telle que celle décrite dans le paragraphe ci-dessus.

Selon l'invention, la carte comporte une zone d'enregistrement non volatile contenant le nombre d'opérations d'un type déterminé effectuées par le titulaire de la carte, ce nombre étant incrémenté lorsqu'une opération de ce type est effectuée mais n'étant pas incrémenté lorsque la carte est utilisée pour des opérations d'un autre type. Par exemple, si la carte doit effectuer des opérations de débit et des opérations de crédit, un compteur spécifique pourra être prévu pour les opérations de crédit seulement; ou encore pour les opérations de débit seulement; ou encore on pourra avoir un compteur séparé pour les

opérations de débit et les opérations de crédit. S lon l'invention des secrets nécessaires pour effectuer des débits seront ainsi différents de ceux nécessaires pour effectuer des rechargements.

Le compteur d'opérations est irréversible, c'est-à-dire que la zone de mémoire est organisée de manière que le contenu lu ne puisse correspondre qu'à un nombre d'unités variant toujours dans le même sens.

Le terminal de lecture de la carte établira et enregistrera dans la carte un certificat résultant d'un algorithme de calcul utilisant d'une part les données d'identification de la carte et d'autre part au moins le contenu d'un compteur d'opérations d'un type déterminé.

L'application la plus simple, dans le cas où les cartes sont rechargées à partir d'un terminal de rechargement, est la suivante : le rechargement n'est effectué que si le certificat inscrit dans la carte est compatible avec les données d'identification de la carte et avec le contenu non volatil du compteur d'opérations de rechargement. On peut ainsi éviter une double opération de rechargement dans des organisations de rechargement en différé. Par exemple, lorsqu'un grand nombre de cartes doivent être rechargées au cours d'une période de temps auprès d'un terminal de rechargement quelconque, il faut éviter qu'une carte ne soit rechargée plusieurs fois dans des terminaux différents au cours de la même période. La présente invention apporte une solution à ce problème. L'enregistrement du certificat dans la carte n'est nécessaire que pour les cartes à mémoire seule. Pour les cartes à micro-processeur, le certificat que transmet le terminal à la carte peut être seulement contrôlé par la carte elle-même qui accepte ou refuse l'ordre en fonction de la véracité de ce certificat.

Le procédé de transaction selon l'invention

comporte donc les opérations suivantes : utilisation de la carte et incrémentation irréversible d'un compteur d'opérations, présent dans la carte, uniquement lorsqu'une opération d'un type déterminé est effectuée au cours d'une utilisation, le compteur n'étant pas incrémenté pour des opérations d'un autre type.

De préférence, l'opération qui donne lieu à incrémentation du compteur d'opérations est une opération de rechargement d'une valeur consommable dans une mémoire de la carte.

On peut prévoir qu'il y a plusieurs compteurs, chacun étant incrémenté pour un type d'opération respectif. On peut même prévoir qu'un compteur est incrémenté pour chacune des opérations appartenant à un groupe de plusieurs types d'opérations différents, ce compteur n'étant pas incrémenté pour d'autres opérations possibles mais n'appartenant pas à ce groupe.

Dans une mise en oeuvre détaillée possible, dans laquelle les cartes sont rechargeables dans des terminaux dispersés susceptibles de recevoir des données d'un serveur, l'invention peut comporter les étapes suivantes :

- chargement, depuis un serveur vers des terminaux de rechargement de cartes, de données permettant aux terminaux de vérifier le droit d'une carte à être rechargée;

- introduction d'une carte dans un terminal de rechargement quelconque;

- lecture par le terminal de données d'identification de la carte présentes dans la carte

- lecture par le terminal d'un compteur d'opérations de rechargement présent dans la carte

- lecture et vérification par le terminal d'un certificat d'authenticité présent dans la carte, ce certificat faisant intervenir les données

d'identification et le contenu du compteur; le compteur d'opérations de rechargement étant incrémenté après chaque opération de rechargement et n'étant pas incrémenté pour des opérations autres qu'un rechargement.

Ces opérations selon l'invention permettent d'établir l'habilitation de la carte.

La vérification de la zone certificat ne doit être faite par le terminal que pour les cartes à mémoire seule, car pour les cartes à micro-processeur la valeur du solde peut être garantie par les mécanismes sécuritaires mis en place pour les débits et les rechargements.

Après ces opérations, le rechargement peut être effectué.

Dans cette définition, on notera que le serveur n'est pas forcément physiquement relié aux terminaux : une disquette de mémoire magnétique produite par le serveur peut être transportée dans les terminaux pour y placer les données nécessaires aux vérifications d'habilitation des cartes.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée qui suit et qui est faite en référence aux dessins annexés dans lesquels :

- la figure 1 représente l'organisation générale d'une application dans laquelle la présente invention peut être avantageusement mise en oeuvre;

- la figure 2 représente schématiquement diverses zones de mémoire non-volatile d'une carte utilisable dans le procédé selon l'invention;

- la figure 3 représente un organigramme général des étapes d'un procédé de rechargement de carte selon l'invention.

L'invention sera décrite en détail à propos d'un exemple d'application particulier (fig 1) qui est la

gestion des cartes de restaurant d'entreprises. Les titulaires des cartes sont des employés appartenant à des entreprises ou organismes différents, la gestion des cartes étant assurée par un prestataire de service (entreprise de restauration).

On suppose que tous les employés d'une entreprise possèdent une carte de type "porte-monnaie électronique" permettant d'accéder au restaurant d'entreprise, le financement de cette carte étant pris en charge par le titulaire et/ou par l'entreprise.

Chaque mois, après avoir payé au prestataire de service une somme correspondant aux cartes à recharger, l'entreprise reçoit du prestataire un fichier contenant tous les ordres de rechargement de ses employés. Ce fichier est destiné à être utilisé par un ou plusieurs terminaux de rechargement 10 placés dans l'entreprise. Si l'entreprise occupe une surface importante plusieurs terminaux seront répartis sur cette surface afin que tous les employés puissent facilement accéder à un terminal le jour où ils doivent effectuer le rechargement de leur carte.

Le fichier de rechargement peut être transmis par le prestataire de service de différentes manières; par exemple la transmission peut se faire par une liaison directe ou une liaison par modem si les terminaux sont reliés directement ou par des lignes téléphoniques à un serveur 20 du prestataire; ou au contraire, la transmission peut se faire par transport physique d'une disquette magnétique 30 ou de tout autre moyen de mémoire non volatile (carte à puce, etc.) si les terminaux ne sont pas reliés au serveur 20 du prestataire.

Le fichier transmis par le prestataire est installé dans les terminaux de rechargement de l'entreprise. Le fichier de rechargement transmis aux terminaux peut être le même pour tous les terminaux. Il

est alors dupliqué dans tous ces terminaux.

Ces terminaux peuvent être de simples ordinateurs personnels (PC) avec un lecteur de cartes à puce.

Les employés désirant recharger leur carte peuvent se rendre auprès d'un terminal quelconque (l'invention permet d'éviter d'obliger un titulaire de carte à utiliser un terminal précis). La carte est introduite dans le lecteur de cartes du terminal 10 et est automatiquement rechargée du montant prévu à l'avance par le prestataire de service, montant qui peut être constant pour tous les titulaires ou au contraire individualisé pour chacun. Le montant peut également varier en fonction de la date du rechargement.

Le prestataire de service gère les montants qui doivent être rechargés dans chaque carte.

La période pendant laquelle peut s'effectuer le rechargement peut être fixe ou variable. Par exemple on peut prévoir que le rechargement doit être effectué le premier de chaque mois.

La carte ainsi rechargée peut être utilisée un certain nombre de fois entre deux rechargements pour consommer les services offerts par le restaurant d'entreprise, selon des modalités définies par le prestataire de service.

La description de l'exemple d'application qui précède permet de mieux comprendre le fonctionnement de l'invention.

Dans le procédé et le système de transaction selon l'invention, la carte comporte des moyens pour compter (et mémoriser de manière non-volatile) le nombre d'opérations de rechargement effectuées, ce compteur n'étant pas incrémenté lors des autres utilisations de la carte, c'est-à-dire en particulier lors de l'utilisation de la carte pour consommer des services.

On remarquera que dans d'autres applications, le

compteur pourrait bien sûr mémoriser un autre type d'opérations que le rechargement: par exemple des opérations de visualisation d'état du compte.

La figure 2 représente schématiquement différentes zones de mémoire non volatile qui peuvent être prévues dans la carte pour mettre en oeuvre l'invention. Ces zones ont été représentées comme différentes parties d'une même mémoire non volatile MNV; mais bien entendu, ces zones de mémoire peuvent être physiquement séparées les unes des autres, c'est-à-dire qu'elles ne sont pas forcément toutes adressables par un même décodeur d'adresse unique. Il faut bien comprendre en effet que ces différentes zones ne sont pas forcément accessibles de la même manière. Par exemple certaines zones, telles que celle qui contient une donnée d'identification de la carte sont complètement inaccessibles en écriture, alors que d'autres (celle qui contient un solde par exemple) peuvent être accédées en écriture.

Sur la figure 2, on a représenté à titre d'exemple une première zone Z1 qui contient les données d'identification (PIN: Personal Identification Number) de la carte; ces données permettent d'identifier de manière univoque la carte, c'est-à-dire qu'il n'y a pas deux cartes ayant les mêmes données d'identification.

Une autre zone Z2 sert de compteur d'opérations de rechargement de la carte et contient un nombre NBR représentant donc le nombre de rechargements déjà effectués. Cette zone est incrémentée à chaque opération de rechargement mais n'est pas incrémentée lorsque la carte est utilisée pour d'autres opérations.

Une troisième zone Z3 contient un certificat CRT qui est une donnée résultant d'un algorithme de sécurité; ce certificat permet de vérifier qu'il n'y a pas d'utilisation non autorisée de la carte, et en particulier qu'il n'y a pas eu des rechargements non autorisés. Cette zone Z3 n'est utile que pour les

cartes à mémoire. En effet pour les cartes à micro-processeur la sécurité est basée sur un certificat ou une signature émis par le terminal à la carte lors d'un débit ou d'un rechargement et qui permet à la carte de vérifier l'origine du débit ou du rechargement.

Une quatrième zone Z4 peut contenir un solde variable SLD, remis à jour au moment du rechargement et diminuant progressivement au fur et à mesure de la consommation de biens ou services à l'aide de la carte.

Une cinquième zone Z5 peut contenir un nombre NOP d'opérations effectuées avec la carte; ce nombre inclut à la fois les opérations de rechargement et les opérations de consommation de biens ou services. Mais la zone Z5 pourrait aussi contenir un nombre NCS représentant seulement les opérations de consommation de biens ou services, cette zone n'étant pas incrémentée lors des opérations de rechargement. En variante, on peut prévoir une zone Z5 pour le nombre NOP et une zone Z6 différente pour le nombre NCS.

Enfin, d'autres zones, référencées globalement sous la référence Z7 peuvent être prévues dans la mémoire MNV.

Pour assurer la sécurité du rechargement, on va s'arranger :

- d'une part pour que seuls soient possibles les rechargements de carte de titulaires autorisés (le prestataire définit les titulaires autorisés, repérés par le numéro d'identification personnelle PIN de la carte);

- d'autre part pour qu'il ne soit pas possible de faire un double rechargement d'une même carte en profitant de la multiplicité de terminaux simultanément préparés pour des rechargements de tous les titulaires.

Pour cela, on utilise à la fois le compteur d'opérations de rechargement présent dans la carte et le numéro d'identification de la carte, également

présent dans la carte. Ces deux données permettent d'établir un certificat, lui aussi plac´ dans la carte, ou au moins contrôlable par la carte, et ce certificat n'est valable que pour une carte déterminée avec un état de compteur déterminé.

L'état NBR du compteur de rechargements (Z2) varie de manière irréversible, c'est-à-dire que le contenu du compteur non volatil (ou le contenu de la zone de mémoire qui constitue ce compteur) représente un nombre entier variant toujours dans le même sens à chaque nouvelle opération de rechargement.

Le protocole de communication entre le terminal de rechargement et la carte peut être celui qui va être décrit ci-dessous; les étapes sont rappelées sur l'organigramme de la figure 3 :

- le titulaire de la carte introduit sa carte dans le terminal de rechargement; les opérations qui suivent peuvent se dérouler automatiquement sans intervention du titulaire, mais on comprendra que dans certains cas on peut préférer une intervention du titulaire (notamment si le terminal est un PC pouvant servir à d'autres usages).

- le terminal lit dans la zone Z1 le numéro d'identification de la carte (PIN);

- le terminal recherche, dans le fichier de rechargement transmis par le prestataire, un numéro correspondant, pour s'assurer que le titulaire fait partie des titulaires a priori habilités;

- le terminal lit dans la carte le contenu NBR du compteur de nombre de rechargements (Z2);

- le terminal lit dans la carte le contenu CRT de la zone de certificat Z3 uniquement si le certificat a été enregistré dans la carte, ce qui n'est nécessaire que pour les cartes à mémoire; le certificat contenu dans cette zone y a été placé lors d'une opération de rechargement précédente;

- le terminal lit dans le fichier de rechargement on calcule, par un algorithme faisant intervenir le numéro d'identification PIN et le contenu NBR du compteur de rechargements, le certificat théorique qui devrait correspondre au numéro d'identification lu et au nombre de rechargements lu; dans une variante préférée d'exécution, le terminal ne possède pas l'algorithme de calcul et il se contente de prélever, dans le fichier de rechargement établi par le serveur, un certificat correspondant à la carte et au numéro d'ordre de l'opération de rechargement; l'avantage de cette manière de procéder est que l'algorithme est alors présent uniquement dans le serveur et n'a pas besoin d'être présent dans les terminaux; ceux-ci ne peuvent être alors détournés par fabrication du fichier de rechargement qui leur est transmis.

- le terminal vérifie la compatibilité du certificat lu et du certificat calculé ou prélevé dans le fichier, et autorise ou non les opérations de rechargement qui suivent en fonction du résultat de la vérification; en cas de non compatibilité, les mesures prises peuvent être diverses, par exemple : rejet de la carte, messages d'erreur, demande de nouvelle tentative, confiscation de la carte au bout de plusieurs tentatives manquées, mise en mémoire, dans un fichier des tentatives de fraude, du numéro de la carte ayant donné lieu à ces échecs, etc.

- pour les cartes à microprocesseur, le terminal envoie à la carte l'ordre avec le certificat de son fichier et la carte autorise ou refuse l'ordre en fonction de la véracité du certificat. Si la carte autorise l'ordre, de façon automatique elle incrémente son compteur de transaction.

- en cas de succès de la vérification, le terminal ou la carte effectuent le rechargement : c'est une remise à jour de la zone de mémoire non volatile Z4

représentant un crédit disponible (en somme d'argent, en unités de compte, en nombre de repas, etc...); au besoin cette mise à jour s'effectue en cumulant les unités apportées au solde des unités présentes dans la carte.

- le terminal incrémente le contenu du compteur d'opérations de rechargement Z2; cette incrémentation peut aussi être effectuée plus tard;

- le terminal inscrit un nouveau certificat dans la zone de certificat Z3 de la carte; ce certificat est calculé par le terminal s'il possède l'algorithme, ou prélevé dans le fichier de rechargement si le terminal ne possède pas l'algorithme; le calcul du certificat fait intervenir l'identification de la carte, et le nouveau contenu du compteur d'opérations de rechargement (ou l'ancien contenu incrémenté d'une unité);

- dans une réalisation possible, la carte possède l'algorithme de calcul du certificat et peut calculer et enregistrer le nouveau certificat et vérifier que le nouveau certificat écrit par le terminal correspond bien à celui qu'elle calcule; sinon, diverses mesures de protection peuvent être prises, telles que par exemple l'absence d'incrémentation du compteur.

La procédure de rechargement se termine alors. La carte ayant subi avec succès la procédure de rechargement peut être utilisée pour des opérations de consommation de biens ou services (consommation de repas dans le restaurant d'entreprise).

Le terminal quant à lui inscrit dans le fichier de rechargement ou dans un autre fichier une information indiquant que pour cette carte le rechargement a été effectué. Cette information sera transmise ultérieurement au serveur chez le prestataire de service.

Si l'utilisateur se présente maintenant à un autre

terminal de rechargement, au cours de la même période de rechargement, avec sa carte déjà rechargée, la procédure de rechargement ne pourra pas à nouveau se dérouler normalement puisque à la fois le contenu du compteur d'opérations et le certificat auront changé. L'irréversibilité du compteur empêche toute fraude : il n'est pas possible de remettre à sa valeur précédente le contenu de la zone Z2 lorsqu'il a changé.

Il peut arriver qu'un utilisateur n'ait pas rechargé sa carte à la fin de la période pendant laquelle le rechargement aurait dû s'effectuer. Dans ce cas, les rechargements suivants deviennent difficiles à gérer.

Pour que cette situation soit plus facilement gérée, on peut prévoir que le fichier de rechargement transmis aux terminaux comporte plusieurs enregistrements pour chaque carte, correspondant l'un à l'opération de rechargement en cours, l'autre aux dernières opérations de rechargement théoriques qui auraient dû être effectuées et qui en fait ne l'ont pas été. Pour un numéro de carte donné, on a donc au moins un enregistrement comportant une information de contenu de compteur correspondant à l'opération théorique en cours, avec un certificat correspondant, mais aussi éventuellement, pour certaines cartes deux enregistrements (ou plus) avec un même numéro de carte, et plusieurs contenus de compteur successifs (autant que d'opérations de rechargement non effectuées), et des certificats correspondants.

Dans ce cas, le terminal recherche toujours l'enregistrement correspondant au nombre de rechargements indiqué dans la carte. En effet, c'est le rechargement correspondant à ce nombre qui doit être fait en premier. Ceux d'avant sont supposés faits puisque la carte a été incrémentée jusqu'à ce contenu; ceux d'après ne doivent être effectués qu'ensuite. La

procédure de rechargement peut alors être effectuée normalement vis-à-vis de cet enregistrement. Lorsqu'elle est effectuée, le titulaire peut procéder à nouveau à un rechargement, par exemple le dernier s'il n'y avait qu'un seul enregistrement de retard. Ce nouveau rechargement peut être effectué dans le même terminal ou un autre.

Dans ce qui précède, on a supposé que le numéro d'identification de la carte et le contenu du compteur de rechargements servent directement à calculer le certificat d'authenticité. Mais on peut prévoir aussi que ces éléments peuvent servir à établir des clés de cryptage des transmissions entre la carte et le terminal et non pas seulement le certificat.

Les étapes principales décrites ci-dessus et rappelées à la figure 3 représentent une procédure simple de transaction; il va de soi que des procédures plus complexes peuvent être mises en oeuvre pour accroître la sécurité; par exemple l'habilitation de la carte peut être renforcée par une procédure de vérification d'un code secret demandé par le terminal et introduit par l'utilisateur sur un clavier du terminal de rechargement.

Pour réaliser un compteur irréversible à partir d'une zone de mémoire Z2, il est classique maintenant d'utiliser des mémoires non-volatiles dont les cellules peuvent être programmées successivement les unes après les autres, l'effacement étant impossible. La programmation peut être effectuée sous la commande d'un microprocesseur lorsque la carte en comporte un, ou sous la commande de circuits simples lorsqu'il n'y a pas de microprocesseur.

Enfin, on comprendra que si la carte comporte plusieurs compteurs pour des types d'opérations différents, tels que ceux qui correspondent aux zones Z2 et Z6, les contenus de chacun de ces compteurs

peuvent servir à des procédures de vérification pour les différents types d'opérations effectuées avec la carte.

On aura compris de l'exemple d'application détaillé ci-dessus que l'invention est particulièrement applicable à un système de gestion collective de nombreux restaurants d'entreprise ayant chacun plusieurs terminaux de rechargement à la disposition des employés de l'entreprise. Elle est en outre aisément transposable à n'importe quel autre type de services.

REVENDICATIONS

1. Procédé de transaction à partir d'une carte à mémoire (40) comportant une mémoire non volatile (MNV), ce procédé comportant l'utilisation de la carte et l'incrémentation irréversible d'un compteur d'opérations présent dans la carte, caractérisé en c que le compteur (Z2) est incrémenté uniquement lorsqu'une opération d'un type déterminé est effectuée au cours d'une utilisation de la carte, le compteur n'étant pas incrémenté pour des opérations d'un autre type.

2. Procédé de transaction selon la revendication 1, caractérisé en ce que l'opération d'un type déterminé est une opération de rechargement d'une valeur consommable dans la mémoire de la carte.

3. Procédé de transaction selon l'une des revendications 1 et 2, caractérisé en ce que plusieurs compteurs (Z2, Z6) sont prévus, chacun étant incrémenté pour une opération d'un type respectif.

4. Procédé de transaction à partir d'une carte à mémoire comportant une mémoire non volatile, comportant l'utilisation de la carte et l'incrémentation irréversible d'un compteur d'opérations, caractérisé en ce que le compteur est incrémenté uniquement lorsqu'une opération appartenant à un groupe d'opérations de types différents est effectuée, le compteur n'étant pas incrémenté pour les opérations d'un type n'appartenant pas à ce groupe.

5. Procédé de transaction dans lequel les cartes sont rechargeables dans des terminaux de rechargement (10) dispersés susceptibles de recevoir des données d'un serveur (20), caractérisé en ce qu'il comporte les

étapes suivantes :

- chargement, depuis le serveur vers les terminaux, de données permettant aux terminaux de vérifier le droit d'une carte à être rechargée;
- introduction d'une carte (40) dans un terminal de rechargement quelconque;
- lecture par le terminal de données d'identification de la carte (PIN);
- lecture par le terminal du contenu (NBR) d'un compteur d'opérations de rechargement (Z2) présent dans la carte;
- lecture et vérification par le terminal d'un certificat d'authenticité (CRT) présent dans la carte, ce certificat faisant intervenir les données d'identification de la carte et le contenu du compteur d'opérations de rechargement, le compteur d'opérations de rechargement (Z2) étant incrémenté après chaque opération de rechargement et n'étant pas incrémenté pour des opérations autres qu'un rechargement.

6. Système de transaction comportant des cartes à mémoire (40) et des terminaux (10) de rechargement de carte, caractérisé en ce qu'il comporte des moyens pour inscrire dans une zone (Z2) de mémoire non volatile de la carte un nombre (NBR) représentant le compte du nombre d'opérations de rechargement effectuées avec la carte, ce nombre étant incrémenté irréversiblement à chaque opération de rechargement et n'étant pas incrémenté pour d'autres opérations effectuées avec la carte.

7. Système selon la revendication 6, caractérisé en ce qu'il est prévu des moyens de vérification de l'habilitation de la carte, ces moyens faisant intervenir des données d'identification (PIN) présentes dans la carte, et le contenu (NBR) de la zone de mémoire (Z2).

8. Système de gestion collective de nombreux

restaurants d'entreprise ayant chacun plusieurs terminaux de rechargement dispersés à la disposition des employés de l'entreprise, caractérisé en ce qu'il utilise le procédé de transaction selon l'une des revendications 1 à 5.

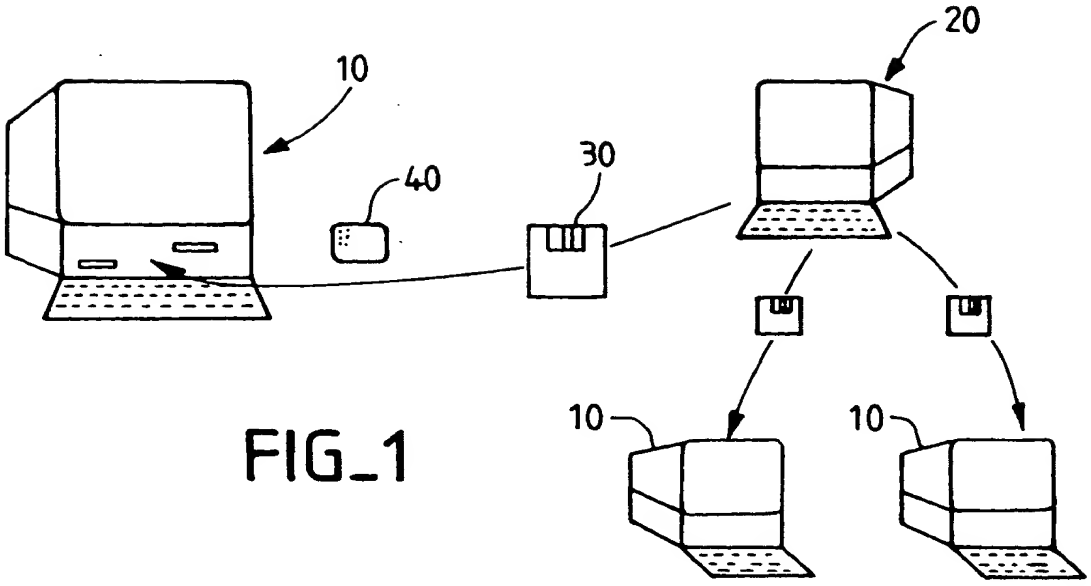

10
20
30
40
10
10

FIG_1

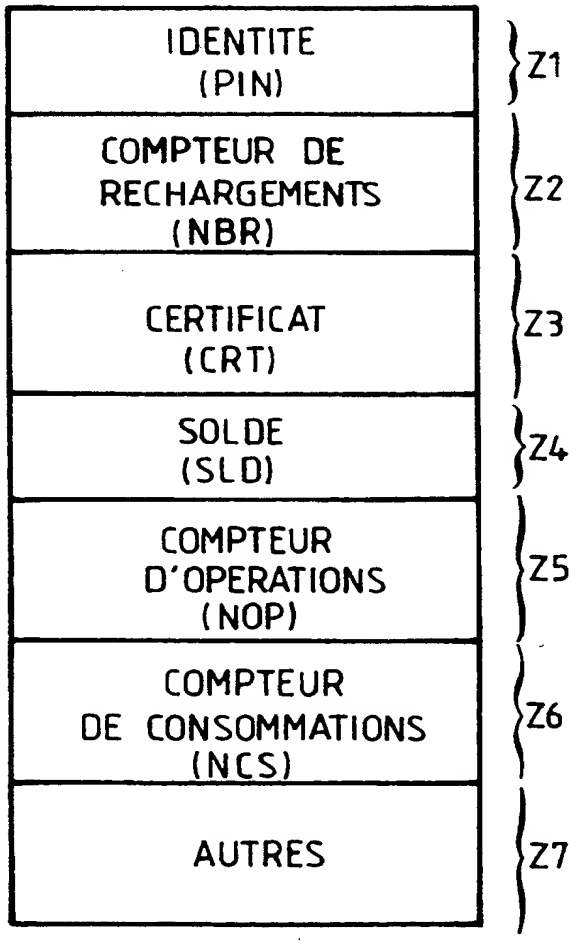
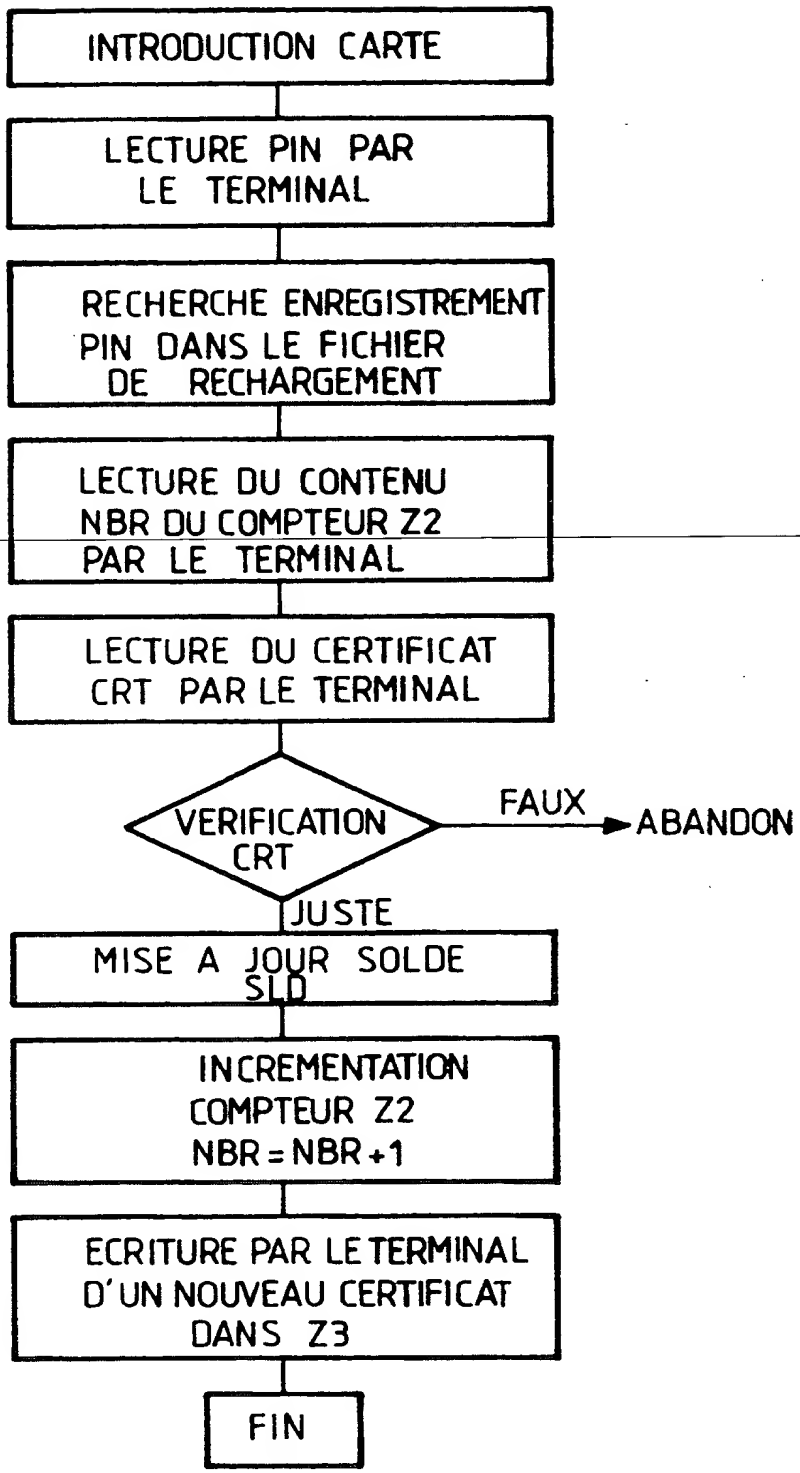

IDENTITE
(PIN)
Z1
COMPTEUR DE
RECHARGEMENTS
(NBR)
Z2
CERTIFICAT
(CRT)
Z3
SOLDE
(SLD)
Z4
COMPTEUR
D'OPERATIONS
(NOP)
Z5
COMPTEUR
DE CONSOMMATIONS
(NCS)
Z6
AUTRES
Z7

FIG_2

FIG_3


INTRODUCTION CARTE
LECTURE PIN PAR LE TERMINAL
RECHERCHE ENREGISTREMENT PIN DANS LE FICHIER DE RECHARGEMENT
LECTURE DU CONTENU NBR DU COMPTEUR Z2 PAR LE TERMINAL
LECTURE DU CERTIFICAT CRT PAR LE TERMINAL
VERIFICATION CRT
FAUX
ABANDON
JUSTE
MISE A JOUR SOLDE SLD
INCREMENTATION COMPTEUR Z2 NBR = NBR + 1
ECRITURE PAR LE TERMINAL D'UN NOUVEAU CERTIFICAT DANS Z3
FIN

REPUBLIQUE FRANÇA

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2716021

N° d'enregistrement national

FA 495885
FR 9401463

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée	
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	EP-A-0 423 035 (GEMPLUS CARD INTERNATIONAL) * colonne 3, ligne 4 - ligne 28 * * colonne 5, ligne 52 - ligne 58 * * colonne 6, ligne 12 - ligne 14; figure 2 * ---	1,4-8	
A	EP-A-0 193 635 (OMRON TATEISI ELECTRONICS CO.) * abrégé * * page 3, alinéa 3 - page 4, alinéa 2; figures 3,4 * ---	1,4-8	
A	FR-A-2 685 520 (MONETEL (SA)) * le document en entier * ---	1,4-6,8	
A	FR-A-2 605 770 (COMPAGNIE GENERALE DAUTOMATISME CGA-HBS) * revendications 1,2; figure 1 * ---	8	
A	EP-A-0 378 454 (GEMPLUS CARD INTERNATIONAL) * colonne 5, ligne 33 - ligne 47; revendication 11 * -----	1,4-6,8	DOMAINES TECHNIQUES RECHERCHES (Int.Cl.5) G06K G07F

Date d'achèvement de la recherche	Examinateur
23 Septembre 1994	Ducreau, F

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)